UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-cv-954-WO-JLW

FARHAD AZIMA, Plaintiff, v. NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC., Defendants.	**PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT**

PRELIMINARY STATEMENT

Defendants' Motion for Summary Judgment (ECF Nos. 379, 380 (collectively, "MSJ")) is unsupported by evidence and foreclosed by the law.

Most summary judgment motions contain a lengthy statement of undisputed facts. Yet Defendants muster fewer than three pages that boil down to two alleged undisputed facts: (1) Azima's rolodex trade secrets were actually created for this litigation; and (2) Azima did not create and therefore does not own the rest of his identified trade secrets. MSJ at 3. As shown below, both points are disputed. *See infra* at 3 n. 1, 22. Defendants' lack of evidentiary support in a complex case alleging misappropriation of 38 trade secrets dooms their Motion.

Defendants attempt to knock out *all* of Plaintiff's 38 trade secrets by ignoring key evidence, including testimony from both Azima and his top

financial advisor, that supports their validity. There is evidence that each of the 38 trade secrets are in fact trade secrets, creating at least a genuine issue of material fact as to each one.

Defendants make a statute of limitations argument that ignores this Court's ruling that the (undisputed) posting of new WeTransfer links publishing Azima's stolen data in 2018 and 2019 restarted the statute of limitations period. *See* ECF No. 65 at 21-24. It also disregards the undisputed fact that Plaintiff learned of the publication in July 2018, within the limitations period.

Defendants' damages and causation arguments concede that Defendants were paid at least $35 million for their work on behalf of Ras Al-Khaimah ("RAK"). Defendants do not dispute Plaintiff's evidence that these payments related to hacking Azima and publishing his trade secrets. The Motion must be denied.

STATEMENT OF FACTS MATERIAL TO DEFENDANTS' MOTION

I. AZIMA'S TRADE SECRETS

Azima is an entrepreneur with 50 years of experience, including many successful business ventures. *See* Ex. 1 at 89:19-90:4. Azima has served as chairman and chief executive for six airlines; created dozens of airlines globally; run an aviation maintenance business; built pilot training centers;

and operated an aircraft leasing business. *Id.* at 155:22-157:3; 183:8-184:7; 158:15-159:4; 196:5-14.

Azima has specialized knowledge and strong business relationships. *See, e.g., id.* at 456:6-457:10; Ex. 2 at 382:2-383:7. Azima's business depends on the trust of the business partners. *See* Ex. 1 at 195:6-196:14.

Defendants did not just misappropriate one trade secret – they stole and misappropriated *all* of Azima's data, containing decades of confidential and proprietary business information. From the stolen data, Azima has identified 38 examples of trade secrets for trial. *See* Ex. 3 at 8-11. These trade secrets include Azima's rolodex, financial forecasts, business plans, and proposals for government contracts and other work. *Id.*

Azima's 38 identified trade secrets ("TS") are valuable. *See* Ex. 2 at 361:2-21; Ex. 53 (TS initialed by Azima's financial advisor). His rolodexes are essential to his business, and the contacts therein have permitted Azima to broker valuable transactions across a variety of industries.[1] *See* Ex. 1 at 294:8-15; 298:13-299:10. They contain key non-public contacts and private contact information in those industries. *See* Ex. 2 at 382:2-383:2. Contacts in these

[1] Defendants wrongly assert that Azima's rolodexes were "created for use in this litigation." MSJ at 3 (emphasis omitted). They were collected from his personal devices and email. *See* Ex. 12-A, ¶ 77. The data itself was not created for the litigation. *Id.*

industries are generally discoverable only by expending significant effort, time, and money. Ex. 3 at 13-14.

Azima's financial forecasts resulted from his unique knowledge and experience. *Id*. at 14. They cannot be easily recreated and reflect specialized knowledge regarding business and revenue generation. *See* Ex. 2 at 291:9-292:5; 293:1-294:4; 374:13-375:2; 375:19-376:11; 380:3-15; Ex. 1 at 171:4-11; 451:14-452:4.

Azima's business plans and proposals reflect his expertise, containing valuable confidential business strategies and industry knowledge not readily ascertainable and only created with great effort, time, and money. *See* Ex. 2 at 381:2-20; Ex. 4 at 220:7-22; Ex. 3 at 14. Several of Azima's trade secrets concern worldwide government contracting issues, deriving value from confidential information reflecting Azima's unique knowledge and experience. Ex. 3 at 14-15.

Azima is the owner of all 38 identified trade secrets. *See* Ex. 1 at 431:12-15, 18-22; 432:1-14; 433:2-3. They involve entities Azima owns in whole or in part. Azima is the sole owner of ALG Transportation, *id*. at 55:17-56:19; Ex. 4 at 22:3-8; the majority shareholder of Shollar Bottling Company, Ex. 1 at 54:1-8; and part owner of Smokehouse BBQ, *id*. at 45:10-22, Aerotech, *id*. at 50:4-6, Caucas International, *id*. at 52:13-17, and HeavyLift International, *id*. at 27:4-12.

These trade secrets reflect Azima's knowledge and expertise, and Azima directed or contributed to their creation. *See id.* at 150:20-152:5; 168:3-15; 169:1-14; 451:6-13; 177:11-16; 177:22-178:11; 186:3-7; 191:9-21; 208:7-20; Ex. 2 at 121:9-22; 119:13-19; 387:12-18; 129:17-130:3; 292:3-13; 375:4-17. They include compilations of data based on his own synthesis and work product. *See* Ex. 1 at 212:6-13; 220:10-221:21; 222:6-9; Ex. 2 at 384:15-385:19.

The trade secrets were maintained electronically on password-protected devices with antivirus software. *See* Ex. 1 at 433:14-22; 420:13-15; 421:1-5; 422:5-423:14; Ex. 2 at 362:2-21; 363:3-5. Azima used password-protected email accounts, which were not accessible to employees. *See* Ex. 1 at 425:14-17; Ex. 2 at 363:6-18. Hard-copy trade secret files were kept under lock and key. *See* Ex. 1 at 109:19-110:1; 88:10-21. Azima's offices were locked and secure. Ex. 2 at 364:3-14. The trade secrets were also subject to additional confidentiality and security measures, including confidentiality labels on the documents themselves, *see* ECF Nos. 382-385 (Defs.' Exs. B-1, B-2, B-4, B-12, B-13, B-16, B-18, B-19, B-24, B-30, B-32, and B-35); confidentiality labels on transmittal emails, *see* Ex. 2 at 373:1-6; 373:15-374:7; ECF Nos. 382-385 (Defs.' Exs. B-6, B-9, B-14, B-24, B-33, B-34, and B-39); and confidentiality or non-disclosure agreements with employees of some of his businesses and with third-party recipients, *see* Ex. 1 at 106:20-107:9; 111:1-9; 127:7-15; 149:12-150:5; 286:3-9; 419:13-420:2. Azima also conducted business with governments that adhere

to strict confidentiality. *See id.* at 32:10-33:21; 60:11-61:20; 187:2-21; 237:22-238:14; 357:10-358:19.

II. DEL ROSSO'S ACQUISITION OF AZIMA'S TRADE SECRETS WITHOUT CONSENT

Beginning in 2014, Defendants and their co-conspirators plotted to hack and steal Azima's confidential business data, including his trade secrets. Ex. 5 at 6 (plan proposing to publish information to "bring legal and public attention against [Azima]"). They did so for RAK in a broad conspiracy to hack RAK victims and weaponize victims' data against them. RAK's law firm, Dechert, retained Del Rosso knowing he previously had been accused of hacking. *See* Exs. 6 & 7.

Defendants then hired CyberRoot (Ex. 8; Ex. 9 at 301:4-11), which Meta determined is a hacking firm. *See* Ex. 10. Defendants admit paying CyberRoot more than $1 million. *See* ECF No. 86, ¶ 29. CyberRoot admits it stole Azima's data on behalf of Defendants. *See* ECF No. 246, ¶¶ 5(a)-(e), 8(d), Ex. A. Expert testimony connects CyberRoot to phishing emails sent to Azima and others. *See* Ex. 11-A ¶¶ 12-13, 29, 90. Defendants also hired hacker Aditya Jain, who attempted to conceal his involvement in hacking Azima at Defendants' request. *See* ECF No. 61 at Ex. 1, pp. 10-15.

It is undisputed that Defendants obtained and still possess Azima's confidential, stolen data, *see* Ex. 9 at 17:6-11; 18:13-19:3, 19:11-13, 22:25-23:6,

without Azima's consent. *See id.* at 18:13-19:13. Cybersecurity expert Christopher Tarbell determined that Defendants presently possess 36 of Azima's 38 identified trade secrets. Ex. 12-A, ¶ 17.

III. DEL ROSSO'S REPEATED PUBLICATION OF AZIMA'S DATA ONLINE

CyberRoot admits it posted Azima's trade secrets online at Defendants' instruction. *See* ECF No. 246, ¶¶ 5(a)-(e), 8(d), Ex. A. In 2016, CyberRoot created websites disparaging Azima. *Id.* The websites contained links to "BitTorrent" sites that purportedly contained Azima's stolen data, though Azima's experts were not able to meaningfully access it. Ex. 12-A, ¶¶ 19-21; Ex. 13, ¶¶ 92(d), 92(j), 114; Ex. 14 at 46:3-8. Defendants and their co-conspirators possessed Azima's data before the sites were created, *see* Exs. 15 & 16, and used the websites to "launder" the data to conceal their involvement. Ex. 17 at 8. Dechert admits that having Azima's stolen data was "unquestionably extraordinarily problematic" and "deeply, deeply troubling." Ex. 18 at 202:2-14.

In July 2018, Azima discovered the websites that contained links to the WeTransfer file-sharing website that included his stolen data. Ex. 1 at 442:14-22, 443:7-13, 471:12-19; Ex. 2 at 393:2-17, 400:18-21; *see also* Ex. 14 at 53:1-11. Azima's data was then publicly accessible for the first time. Ex. 1 at 471:12-19.

New WeTransfer links containing Azima's stolen data were added to the anti-Azima websites again in June 2019 – as confirmed by RAK's expert. Ex. 19, ¶ 79; *see also* Ex. 14 at 178:18-179:13. Additional anti-Azima sites containing links to the stolen data proliferated for years. *See* Ex. 19, ¶ 78; Ex. 11-A, ¶¶ 12, 70. These sites were part of "a coordinated campaign against Azima" by a group that "sought to share Azima's data with public audiences and publish negative content." *See* Ex. 11-A, ¶ 70.

IV. DEL ROSSO'S IMPROPER USE OF AZIMA'S TRADE SECRETS TO INSTIGATE LAW ENFORCEMENT INVESTIGATIONS

Defendants and their co-conspirators also disclosed Azima's stolen trade secrets to U.S. law enforcement to instigate criminal investigations. Beginning in 2015, Dechert directed Defendants to "investigat[e] and report[]" on supposed misconduct by "Azima, . . . and related business entities and associates" to law enforcement. Ex. 20 at 1; Ex. 21 at 39:7-16. Defendants hired attorney Chris Swecker to interact with law enforcement about Azima. Ex. 20; Ex. 21 at 39:7-16

Defendants also hired Northern Technology, Inc. ("NTi") to analyze the stolen data, *see* Exs. 22 & 23, and directed it to provide Azima's stolen data to law enforcement. Ex. 24 at 312:9-313:19; Ex. 22. NTi created reports about Azima's stolen data from August 2016 through early 2020, *see* Ex. 24 at 316:4-

22., and gave the FBI "documents over all the course of the investigation." Ex. 25 at 137:1-8.

NTi also provided law enforcement with Azima's business and banking contacts. Ex. 24 at 293:22-294:5; *see also* Ex. 21 at 213:3-24; Exs. 26-28. The FBI interviewed people based on the contacts NTi provided. *See* Ex. 25 at 134:24-135:5.

From October 2017 to March 2020, NTi gave thousands of Azima's documents to the FBI.[2] *See* Exs. 30-33, 36. Defendants' co-conspirators held at least seven meetings, briefings, or presentations with law enforcement to discuss Azima and his stolen data. *See* Exs. 34-42. The stolen data provided to the FBI contained several exact or near matches of most of Azima's 38 identified trade secrets. Ex. 12-A, ¶ 17(c).

V. AZIMA'S FINANCIAL HARM AND DEL ROSSO'S ILLEGAL GAIN

Azima was harmed by Defendants' misappropriation. After his trade secrets were published in 2018, banks closed Azima's accounts and refused to finance his projects, Ex. 1 at 444:15-445:1; business partners canceled contracts, *id.* at 444:2-14; and Azima was unable to generate new business, *id.* at 486:9-487:22. Azima's "ability to do business . . . was hampered substantially when banks backed out of deals." Ex. 2 at 382:2-384:13; *see also*

[2] Dechert drafted grand jury subpoenas to NTi seeking Azima's documents. *See* Ex. 29.

Ex. 43 ([redacted]).

Defendants reaped a windfall for stealing and using Azima's trade secrets. They received $35 million from RAK for work related at least in part to Azima, *see* Ex. 44 at 71:1-72:3; Ex. 9 at 237:5-11, and to disclose Azima's data to law enforcement. *See* Exs. 45-46, 36. Defendants received $23.9 million from October 2017 forward, within the limitations period. Ex. 47-A (Ex. A at 3-4).

Defendants do not rebut Azima's evidence that the $35 million they received was for criminal misconduct related to the conspiracy to injure Azima. MSJ at 27-28. Defendants have refused to produce any documentation regarding the $35 million. Forensic accounting expert Jimmy Pappas found that Defendants' financial records were not "complete financial records, typically retained by business organizations . . . ." Ex. 47-A, ¶ 20. Pappas concluded that Azima is entitled to disgorge the $35 million Defendants received. *Id.* ¶ 11. Defendants did not present a rebuttal expert on disgorgement.

VI. DEFENDANTS' SCHEME TO DESTROY EVIDENCE

Defendants and their co-conspirators repeatedly destroyed evidence. CyberRoot admits Del Rosso ordered it to destroy its work product for Defendants right after Azima filed this case. *See* ECF No. 246, ¶ 8(f). [redacted]

[redacted] *See* Ex. 8, ¶ 4.

Defendants also lied about the purpose of payments to their co-conspirators. They manufactured false engagement letters with hackers. ECF No. 61 at Exs. 1, 2. They attempted to destroy 100,000 documents from Del Rosso's laptop the night before he testified about his acquisition and use of Azima's stolen data. Ex. 48, ¶¶ 8.2.1., 8.2.4, 8.2.6. Defendants' co-conspirators destroyed work product or transferred documents out of the U.S. on the eve of this lawsuit. *See* Ex. 49 ([redacted]); Ex. 50 [redacted]); Ex. 51 (Dechert sent the stolen Azima data it produced to law enforcement to RAK in 2020).

STANDARD OF REVIEW

Courts may only grant summary judgment "when, viewing the facts in the light most favorable to the non-moving party, there is no genuine issue of any material fact and the movant is entitled to judgment as a matter of law." *Static Control Components, Inc. v. Darkprint Imaging, Inc.*, 200 F. Supp. 2d 541, 543-44 (M.D.N.C. 2002) (citations omitted). The moving party "bears the burden of initially . . . demonstrating the absence of a genuine issue of material fact." *BSN Med., Inc. v. Parker Med. Assocs. LLC*, No. 3:09-CV-00015-MOC-DSC, 2011 WL 5509030, at *17 (W.D.N.C. Nov. 17, 2011).

Where there is a dispute of fact about the validity of trade secrets, courts have denied defendants' motions for summary judgment in North Carolina Trade Secret Protection Act ("TSPA") cases. *See, e.g., Static Control Components, Inc.* 200 F. Supp. 2d 541 at 546 (denying defendants' summary judgment motion under the TSPA because a genuine issue of material fact existed); *BSN Med.*, 2011 WL 5509030, at *1 (same); *Decision Insights, Inc. v. Sentia Grp., Inc.*, 416 F. App'x 324, 332 (4th Cir. 2011) (same).

ARGUMENT

I. DEFENDANTS' STATUTE OF LIMITATIONS ARGUMENT FAILS AS A MATTER OF LAW AND FACT.[3]

The Court has already dismissed the same statute of limitations argument Defendants make here, holding that the "misappropriation of Plaintiff's trade secrets in 2016 and the more recent misappropriations in 2018-2019, 'give[] rise to multiple discrete claims corresponding to each act of misappropriation, and [b]ecause each act violates the law on its own, each act separately triggers its own limitations period.'" ECF No. 65 at 22 (quoting *Heraeus Med. GmbH v. Esschem, Inc.*, 927 F.3d 727, 737 (3d Cir. 2019)). The law of the case therefore forecloses Defendants' statute of limitations argument because the Court has already ruled that new publications in 2018 and 2019

[3] The statute of limitations runs back three years, to at least October 2017. *See* ECF No. 1 (filed Oct. 15, 2020).

triggered the limitations period anew. *Carlson v. Bos. Sci. Corp.*, 856 F.3d 320, 325 (4th Cir. 2017) ("[W]hen a court decides upon a rule of law, that decision should continue to govern the same issues.") (cleaned up).

None of the facts have changed since the Court's ruling. It is undisputed that Azima did not discover that his stolen data was posted on WeTransfer until July 2018, within the limitations period. *See* Ex. 1 at 442:14-22; 443:7-13; 471:12-19; Ex. 2 at 393:2-17; 400:18-21; *see also* Ex. 14 at 53:1-11. For this reason alone, Defendants' statute of limitations argument fails.

It is also undisputed that new links to Azima's data were published on anti-Azima blog sites in 2019. *See* ECF No. 379 (Defs.' Ex. I-1, ¶ 66) (acknowledging the 2019 website publicizing Azima's data); Ex. 14 at 197:3-10 (same). Defendants' sole challenge to the 2019 disclosure is hotly contested. They argue it "*may have*" only *re*disclosed data that was originally posted outside of the limitations period. MSJ at 9. But they cite no evidence, and indeed, admit it is not clear what information was accessible through that 2019 link. *Id.* (citing Defs.' Ex. H at 197:5-198:20). The 2019 redisclosure in any event made Azima's data newly available, creating new harm when it was published.

There is also a material dispute about when WeTransfer links were first published on anti-Azima websites. Defendants cite Mr. Tarbell's prior statement that Azima's data was "at least initially *uploaded to WeTransfer* on

or about January 27, 2017." Defs.' Ex. H, ¶ 117 (emphasis added); *see also id.* ¶ 124. But when data was uploaded to WeTransfer says nothing about when it was published or otherwise made publicly available. *See* Ex. 12-B, ¶¶ 5-8; Ex. 12-A, ¶¶ 22-26. A data upload creates a link, but the data is not published until the person who uploaded the data sends or posts links to the data. *Id.*; Ex. 14 at 47:9-20.

Defendants continue to misrepresent Mr. Tarbell's conclusions regarding when Azima's data became publicly available. *See*, *e.g.*, Ex. 14 at 47:9-12 ("Q. Okay. So when you say 'uploaded,' you were distinguishing between when the data was uploaded and when it was available?' A. Correct."). Mr. Tarbell has *never* concluded that the links to Azima's data were publicly available in 2017. *See id.* at 46:20-47:20.

The evidence shows that websites disparaging Azima were updated to include such links on or about July 2018. *Id.* at 46:3-8; Ex. 12-A, ¶ 21. Those websites did not include WeTransfer links when they were initially created in 2016. Ex. 12-A, ¶¶ 18-19. Defendants' own expert admits it is no longer possible to determine when the websites were modified to add the WeTransfer links. *See* ECF No. 379 (Defs.' Ex. I-1, ¶ 64). Accordingly, there is at least a material dispute as to when Azima's data became publicly available.

Defendants and their co-conspirators also disclosed Azima's stolen trade secrets to and met with law enforcement numerous times, creating new

injuries within the limitations period. *Supra* pp. 8-9. These ongoing injuries to Azima also preclude summary judgment.

II. DEFENDANTS CANNOT SHOW THAT THERE IS NO GENUINE DISPUTE ABOUT THEIR MISAPPROPRIATION OF AZIMA'S TRADE SECRETS.

A. North Carolina Law Requires a Fact-Specific, Holistic Analysis of Trade Secrets.

The TSPA allows owners to recover damages for misappropriation of their trade secrets. N.C. Gen. Stat. § 66-153. A trade secret is defined as a "business or technical information" that "derives independent actual or potential commercial value from not being generally known or readily ascertainable through independent development or reverse engineering" and "[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." *Id.* § 66-152(3).

North Carolina courts apply a fact-specific analysis in determining whether information constitutes a trade secret – making those issues ill-suited for summary judgment. *Jacobs Vehicle Sys., Inc. v. Zhou Yang*, No. 1:12CV181, 2015 WL 4622734, at *7 (M.D.N.C. Jul. 31, 2015) ("Whether or not a trade secret exists is a fact-intensive question to be resolved at trial.") (cleaned up).

Some courts weigh six fact-based factors,[4] *see, e.g., Sunbelt Rentals, Inc. v. Head & Engquist Equip., L.L.C.*, 174 N.C. App. 49, 53, 620 S.E.2d 222, 226 (2005), while others look to the plain language of the statute, *see, e.g.*, *Bank Travel Bank v. McCoy,* 802 F. Supp. 1358, 1360 (E.D.N.C. 1992). Where courts do weigh the six factors, they need not consider all of them. *See Computer Design & Integration, LLC v. Brown*, Mecklenburg Cnty. No. 16CVS11847, 2017 WL 442691, at *9 (N.C. Super. Ct. (Bus. Ct.) Jan. 27, 2017).

B. Azima Has Sufficiently Established 38 Identified Trade Secrets.

There is no basis to grant summary judgment regarding any of Azima's 38 identified trade secrets. Each of Azima's trade secrets was created through the expenditure of substantial time and money, has commercial value, and was protected as confidential.[5] At a minimum, this evidence creates a genuine dispute of material facts.

---

[4] The six factors include: (1) the extent to which information is known outside the business; (2) the extent to which it is known to employees involved in the business; (3) the measures taken to guard its secrecy; (4) the value of the information; (5) the amount of effort or money expended to develop it; and (6) how difficult it would be to acquire or duplicate the information. *Sunbelt Rentals, Inc. v. Head & Engquist Equip., L.L.C.*, 174 N.C. App. 49, 53, 620 S.E.2d 222, 226 (2005).

[5] Azima does not concede that application of the six-factor test is required, but notes that Defendants' analysis does not address all six factors. Accordingly, Azima addresses only the deficiencies alleged by Defendants.

1. Azima spent substantial time and money to develop his trade secrets.

Evidence shows that Azima expended significant time and money to develop his trade secrets based on his 50 years of industry experience and knowledge. Ex. 1 at 431:18-22; 432:1-14; 433:2-3; 155:22-157:3. He spent effort and time drafting, revising, and compiling the information in the trade secrets. *See, e.g., id.* at 163:1-14; 179:12-15, 21; 224:1-3; 294:8-15; Ex. 4 at 151:7-12; 151:20-152:4; Ex. 2 at 386:1-22; 382:2-383:2; 375:19-377:17.

2. Azima's trade secrets were valuable.

Azima has presented clear evidence that each trade secret had actual or potential commercial value when it was created and misappropriated. *See* Ex. 2 at 361:2-21; Ex. 3 at 13-15; *see also* Ex. 2 at 380:3-15; 278:2-14; 285:3-14; Ex. 1 at 173:20-174:10; 451:14-452:4; 457:8-10; Ex. 4 at 220:7-22. Azima's trade secrets captured knowledge, methodologies, and strategies with continued actual and potential value to his competitors and were valuable in his own work in the aviation industry through 2018. Ex. 1 at 445:15-17; Ex. 3 at 13-15.

Defendants claim that some trade secrets lost *all* value if the related business entity ceased operations, or if the business proposals fell through. MSJ at 14-17. They also claim that certain of Azima's trade secrets contain "stale" information, rendering them worthless. *Id.* But North Carolina courts

have held that historical data can have value and qualify as a trade secret. *See, e.g., Byrd's Lawn & Landscaping, Inc. v. Smith*, 142 N.C. App. 371, 376, 542 S.E.2d 689, 692 (2001) (finding cost history records to constitute "a compilation of information, method, technique, or process" with value to the plaintiff and potential value to plaintiff's competitors). Defendants' case law does not change this conclusion.[6]

3. Azima maintained the secrecy of his trade secrets

Azima took "efforts that are reasonable under the circumstances" to maintain the secrecy of his trade secrets. N.C. Gen. Stat. § 66-152(3)(b). Azima and his financial advisor took steps to protect the confidentiality of each trade secret, Ex. 1 at 433:4-22; Ex. 2 at 362:1-6; Ex. 3 at 15-16, including by:

- Maintaining trade secrets on password-protected devices with firewalls, anti-virus, and anti-malware software. Ex. 1 at 433:14-22; 420:13-15; 421:1-5, 13-17; 422:5-423:14. Ex. 2 at 362:8-21. These

[6] Defendants' cases are inapposite. Most deal with injunctions and none of their cases say historical information cannot have value. *See Philips Elecs. N. Am. Corp. v. Hope,* 631 F. Supp. 2d 705, 723 n.11 (M.D.N.C. 2009) (declining to consider old information as evidence the company did not protect its confidential information); *Merck & Co. v. Lyon*, 941 F. Supp. 1443, 1461 (M.D.N.C. 1996) (finding trade secrets did not meet injunction standard, not that they did not have value); *Health Care Facilities Partners, LLC v. Diamond*, No. 5:21-CV-1070, 2023 WL 3847289, at *16 (N.D. Ohio Jun. 5, 2023) (plaintiffs presented "no evidence, argument, or legal theory" on the value); *UTStarcom, Inc. v. Starent Networks, Corp.*, 675 F. Supp. 2d 854, 871 (N.D. Ill. 2009) (declining to issue injunction because court did not want to "assume value"); *MicroStrategy, Inc. v. Bus. Objects, S.A.*, 661 F. Supp. 2d 548, 554-57 (E.D.Va. 2009 (lifting a five-year-old injunction protecting sales strategies for completely obsolete product).

devices were kept secure, not accessible to others including employees. Ex. 2 at 362:22-363:5; Ex. 1 at 423:8-12.

- Using password-protected email accounts to transmit trade secrets that no one else had access to. Ex. 1 at 434:11-435:1; Ex. 2 at 363:6-18.

- Protecting physical offices with locks, security cameras, and alarms. Ex. 2 at 364:3-14.

- Sharing trade secrets only with authorized third parties within Azima's circle of trust. Ex. 1 at 435:14-436:8; 468:7-17; 437:9-19; 79:16-80:12; 105:5-106:19; 190:21-191:8; 217:18-219:10; 232:13-18; 266:1-20; 270:14-20; 277:12-18; 303:9-14; 314:7-14; 334:21-335:22; 349:10-21; 193:12-194:10; Ex. 2 at 365:2-20; 369:7-10, 18-21; 230:7-13; 238:2-7; 255:5-8; 337:5-11; Ex. 4 at 67:11-18.

- Marking trade secrets as confidential. *See* Defs.' Ex. B at Trade Secrets Nos. 1, 2, 4, 30, 32, 12, 13, 16, 18, 19, 35, and 24.

- Transmitting trade secrets in emails that included confidentiality labels and based on confidentiality agreements. *See* Ex. 2 at 373:1-6; 373:15-374:7; Defs.' Ex. B at Trade Secrets Nos. 6, 9, 33, 14, 34, 24, and 39; Ex. 1 at 106:20-107:9; 111:1-9; 149:12-150:5; 286:3-9; 419:13-420:2.

- Conducting business with the U.S. government, which applied strict confidentiality. *See* Ex. 1 at 32:10-33:21; 60:11-61:20; 187:2-21; 237:22-238:14; 357:10-358:19.

This list of measures rebuts Defendants' unsupported claim that Azima undertook "virtually no measures" to protect confidentiality. *See* MSJ at 19. More than that, Azima's protective measures worked. Other than Defendants and their co-conspirators, Azima is unaware of any other unauthorized access or distribution of any of his trade secrets. Ex. 1 at 436:9-18; Ex. 2 at 365:22-366:12.

The TSPA only requires confidentiality "efforts that are reasonable under the circumstances." N.C. Gen. Stat. § 66-152(3)(b). Even Defendants concede that whether those efforts are reasonable is "often appropriate for resolution by a jury." MSJ at 18-19. Defendants cherry-pick excerpts from cases and testimony, *id.* at 20-24, but courts have clearly held that confidentiality must be evaluated holistically. *See, e.g.*, *Safety Test & Equip. Co. v. Am. Safety Utility Corp.,* Cleveland Cnty., 2015 WL 1880769, at *10 (N.C. Super. Ct. (Bus. Ct.) Apr. 23, 2015) ("The inquiry must be as to specific facts which vary from case to case.").

For example, Defendants claim Azima's password protection is categorically insufficient, (MSJ at 20, 22), but courts have held otherwise. *See, e.g., Am. Circuits, Inc. v. Bayatronics, LLC,* Mecklenburg Cnty. No. 22CVS2915, 2023 WL 8597896, at *9-10 (N.C. Super. Ct. (Bus. Ct.) Dec. 8, 2023). And unlike the trade secrets in Defendants' cited cases,[7] Azima's trade

[7] *See, e.g.*, *Prairie Field Servs., LLC v. Welsh*, 497 F. Supp. 3d 381, 396-97 (D. Minn. 2020) (password protection insufficient where all employees could access trade secrets); *Safety Test & Equip. Co.*, 2015 WL 1880769, at *5, *10 (documents were accessible to most employees, not limited to top-level employees); *McKee v. James*, Robeson Cnty. No. 09-cv-3031, 2013 WL 3893430, at *13 (N.C. Super. Ct. (Bus. Ct.) Jul. 24, 2013) (password protected financial records that were *not identified as trade secrets* could not save trade secrets that were not themselves password-protected).

secrets were stored on a limited number of password-protected devices, not on broadly accessible company networks. *See supra* pp. 5-6.

Defendants also wrongly claim that trusted relationships based on confidentiality are categorically legally insufficient. MSJ at 21, 23. But even Defendants' cases do not rule out that long-running, trusted relationships can preserve secrecy.[8] The facts surrounding Azima's relationships must be considered when evaluating whether his efforts to preserve confidentiality were "reasonable under the circumstances." Such a fact-intensive inquiry creates a genuine issue of material fact by itself.

4. Azima has an ownership interest in all 38 identified trade secrets

Some of the 38 identified trade secrets Azima owns outright. *Supra* pp. 4. Others, he has a stake in via his ownership of entities associated with the trade secrets. *Id.*; *see also* Ex. 1 at 431:12-15, 18-22; 432:1-14; 433:2-3; 466:1-4; Ex. 2 at 360:10-21; Ex. 3 at 12-13; *see also* Ex. 1 at 208:7-20 (TS 7 – Azima contributed input on financing and operations); *id.* at 212:6-15 (TS 8 – Azima

[8] *See Krawiec v. Manly*, 370 N.C. 602, 612, 811 S.E.2d 542, 549 (2018) (sharing a trade secret "in confidence" with employees who had worked with a company for less than a year insufficient); *Campbell Sales Grp., Inc. v. Niroflex ex rel. Jiufeng Furniture, LLC*, Brunswick Cnty. No. 19CVS865, 2022 WL 17413381 at *10 (N.C. Super. Ct. (Bus. Ct.) Dec. 5, 2022) (finding that plaintiff failed to identify <u>any</u> confidentiality efforts); *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) (opining on constitutional questions over a decade before TSPA enactment, *not* analyzing trade secret disclosure for waiver issues).

contributed to the compilation of information); *id.* at 302:4-12; 303:15-304:10; 307:8-19 (TS 23 – reflects input from Azima); *id.* at 326:4-327:8 (TS 31 – compiled at Azima's direction, and reflects his input); *id.* at 347:6-349:9 (TS 35 – includes input from Azima). In each instance, it was Azima who directed and oversaw the creation of the specific trade secrets.

Defendants identify a set of trade secrets they claim belong to other entities. However, the TSPA expressly permits a trade secret to be developed, used, or owned by more than one person. N.C. Gen. Stat. § 66-152 (trade secret protection not lost just "because the information comprising the trade secret has also been developed, used, or owned independently by more than one person, or licensed to other persons."). Whether certain trade secrets "were created by others and concern their businesses," MSJ at 11 (emphasis omitted), has no bearing on whether they constitute trade secrets.

C. Defendants Misappropriated Azima's Trade Secrets.

Defendants misappropriated each of Azima's identified trade secrets. *See id.* at 11.[9] Defendants admit that they possess Azima's stolen data containing his trade secrets and had no permission to obtain it. *Supra* pp. 6-

[9] Misappropriation is defined as, "acquisition, disclosure, or use of a trade secret of another without expressor implied authority or consent." N.C. Gen. Stat. § 66-152(1). Defendants do not seriously contest misappropriation based on this definition, nor could they.

7. Defendants were behind the posting on WeTransfer and oversaw efforts to provide the data to the FBI. *Supra* pp. 7-8.

Cybersecurity expert Christopher Tarbell concluded that 28 of the 38 trade secrets were posted on WeTransfer in 2018 and were provided to the FBI. Ex. 12-A, ¶¶ 17(b)-(c). Of the remaining 10 trade secrets, 6 were contact lists, portions of which were contained in Defendants' data and turned over to the FBI, just in a different format. *Id.* ¶ 17(c) (TS 20, 21, 26, 27, 28, 29). Mr. Tarbell also located different versions of two trade secrets (TS 1 and 2) – financial forecasts and models for HeavyLift – in both the 2018 WeTransfer data and FBI data. *Id.* ¶¶ 17(b)-(c).

D. Azima Did Not Concede Trade Secrets 14 and 36.

Defendants misrepresent Azima's testimony, claiming that Azima "admitted" that TS 14 and 36 are not trade secrets. *See* MSJ at 10. This testimony was taken out of context. *See* Ex. 1 at 255:1-15 (responding to a question as to why he shared TS 14 with a business contact – because it was a business proposal – and not whether he viewed it as a trade secret); *id.* at 355:3-15 (clarifying that TS 36 is a compilation that must be considered in its totality). Azima has maintained that TS 14 and 36 do constitute trade secrets, via sworn interrogatories and testimony. *See id.* at 430:12-431:22; Ex. 3 at

7-11. At most, Defendants have presented a factual dispute as to whether TS 14 and 36 constitute trade secrets.

III. PLAINTIFF HAS SUFFICIENTLY SHOWN CAUSATION.

Azima has established that Defendants' misappropriation of his trade secrets and conspiracy to do so proximately caused his injury. Under the North Carolina trade secrets statute, "damages may . . . be measured by the economic loss ***or*** the unjust enrichment caused by misappropriation of a trade secret." N.C. Gen. Stat. § 66-154(b) (emphasis added).

It is undisputed that Defendants' misappropriation proximately caused their unjust enrichment. Defendants received $35 million for "Project Nariman," which included the scheme to damage Mr. Azima using his confidential data. *See* Ex. 47-A at ¶ 11; *see also* Ex. 44 at 71:1-72:3; Ex. 9 at 237:5-11.

Regardless, Azima did suffer losses as a proximate cause of Defendants' misappropriation and conspiracy. Longtime banking partners closed his accounts, pulled out of deals, and terminated their relationships with him after his trade secrets were published online. Ex. 1 at 443:21-445:1; Ex. 2 at 382:2-384:13. The sudden extinguishment of financing made it impossible for Azima to do business and caused deals to fall through. Ex. 2 at 382:2-384:13.

Finally, Defendants cite a misleading portion of Azima's testimony to inaccurately imply that his harm occurred in 2016. They ignore his other

testimony clarifying that the harm he endured occurred from 2018 forward. *See, e.g.*, Ex. 1 at 487:5-488:8. "Foreseeability is . . . a requisite of proximate cause." *Hairston v. Alexander Tank & Equip. Co.*, 310 N.C. 227, 233, 311 S.E.2d 559, 565 (1984). And here it was only foreseeable Azima would suffer economic harm after Defendants publicly posted his trade secrets online. Prior to 2018, Azima's data was not publicly available, and therefore he could not have been harmed. *Supra* pp. 7-8. While Defendants and Dechert could access the stolen data, none of Azima's competitors or business relations could. At the very least, a genuine dispute exists as to whether Defendants proximately caused Azima's injuries.

IV. AZIMA'S DISGORGEMENT CALCULATION IS NOT SPECULATIVE.

Defendants failed to produce *any* evidence explaining the $35 million it received as a result of the scheme to injure Azima, or to rebut Azima's evidence about that scheme.[10] Ex. 47-A, ¶¶ 15-21; Ex. 52 at 47:20-24; 46:16-24; 65:10-66:1. As a result, Defendants have no evidence to show why they were paid this massive amount or what they did with it. Defendants have thus failed to meet their "initial burden under Rule 56 [to] point[] to undisputed evidence that [they] did not earn a profit." *Next Advisor Continued, Inc. v. LendingTree,*

[10] To the contrary, Defendants affirmatively destroyed documents evidencing the work they and their co-conspirators did. ECF No. 246, ¶ 8(f).

Inc., Mecklenburg Cnty. No. 15CVS21379, 2017 WL 2590777, at *5 (N.C. Super. Ct. (Bus. Ct.) Jun. 14, 2017).

The fact remains that Defendants reaped more than $35 million from RAK. *See* Ex. 47-A at 3; Ex. 44 at 71:1-72:3; Ex. 9 at 237:5-11. They do not contest that they received the funds for the hacking and stealing of Azima's data. *See* MSJ at 28. Disgorgement "is an imprecise science," but it is enough that Azima has given "a reasonable approximation" of the amount to be disgorged. *U.S. Dep't of Hous. & Urb. Dev. v. Cost Control Mktg. & Sales Mgmt. of Va., Inc.*, 64 F.3d 920, 927 (4th Cir. 1995).

Defendants' argument that Azima's *whole case* must be dismissed because his disgorgement calculation extends beyond the 2018 and 2019 WeTransfer[11] ignores that Plaintiff has two claims—misappropriation and conspiracy. The payments leading up to the 2018 and 2019 misappropriations are, at a minimum, recoverable as proceeds of the conspiracy. *New Friendship Used Clothing Collection, LLC v. Katz*, Wake Cnty. No. 16CVS14819, 2017 WL 3601714, at *16 (N.C. Super. Ct. (Bus. Ct.) Aug. 18, 2017); *see also* Restatement (Third) of Torts, Liab. for Econ. Harm § 27 cmt. a (Am. L. Inst. 2020).

[11] Defendants advance this as a causation argument, but "it is well established that experts on damages can assume causation." *Indect USA Corp. v. Park Assist, LLC*, No. 3:18-cv-02409-BEN-DEB, 2021 WL 4311002, at *3 (S.D. Cal. Sept. 22, 2021) (collecting cases).

Even if those payments leading up to the misappropriations were not recoverable, the relevant disgorgement period for Azima's misappropriation claim is a material dispute. At least some of the $35 million was paid for the 2018 and 2019 misappropriation. Defendants billed to Project Nariman in 2018 and 2019, *see* Exs. 45, 46, and CyberRoot worked for (and therefore must have been paid by) VMS and on behalf of Dechert in 2018, 2019, and 2020. *See* Ex. 9 at 121:6-21; 310:10-13. Defendants received $14.4 million in 2018 and 2019 alone. Ex. 47-A (Ex. A, at 3-4). Plaintiff has met his burden; the jury should determine the amount of the harm. *See* Fed. R. Civ. P. 56(c); *Cost Control Mktg.*, 64 F.3d at 927.

Finally, whether the $35 million should be subject to offset is also a factual dispute. Defendants' proceeds are not offset by the amount paid to co-conspirators. Restatement (Third) of Torts § 27 cmt. a ("Each [co-conspirator] is [] liable for damage caused by torts that the other [co-conspirators] commit[]."). Defendants' co-conspirators received these payments for their role in the conspiracy: CyberRoot admits it received $2.3 million to hack Azima and publish his trade secrets, *see* ECF No. 246, ¶ 8(a), (b), (d), (e); Defendants paid Swecker to turn over Azima's stolen data to law enforcement, Ex. 21 at 163:3-14; Ex. 20; and Defendants paid NTi to mine, analyze, and weaponize Azima's confidential data, Ex. 44 at 372:24-373:13; 374:4-9; Ex. 9 at 243:6-16;

319:10-17. Thus, there is a material dispute as to whether any amount should be offset.[12]

V. AZIMA'S CIVIL CONSPIRACY CLAIM IS ACTIONABLE.

Defendants' sole basis for seeking dismissal of Azima's conspiracy claim is that his underlying misappropriations claim purportedly fails. But because Defendants' summary judgment motion as to Azima's misappropriation claim lacks merit, their argument for dismissing Azima's conspiracy claim likewise lacks merit.

CONCLUSION

For the reasons above, Defendants' motion for summary judgment should be denied.

[12] Defendants argue that Mr. Pappas's offset calculation should not include payments to Defendants' counsel. *See* Ex. 47-A, ¶ 22. Defendants' attorneys were used as a conduit for payments to co-conspirators. *See, e.g.*, ECF No. 125 at 7, 13. If proven at trial, such payments would be subject to disgorgement.

This, the 14th day of August, 2024.

WOMBLE BOND DICKINSON (US) LLP

/s/ Ripley Rand
Ripley Rand (N.C. State Bar No. 22275)
Christopher W. Jones (N.C. State Bar No. 27265)
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Telephone: (919) 755-2100
Facsimile: (919) 755-2150
Email: ripley.rand@wbd-us.com
chris.jones@wbd-us.com

MILLER & CHEVALIER CHARTERED

Kirby D. Behre (*pro hac vice*)
Timothy P. O'Toole (*pro hac vice*)
Lauren Briggerman (*pro hac vice*)
Ian Herbert (*pro hac vice*)
Calvin Lee (*pro hac vice*)
Cody Marden (*pro hac vice*)
900 Sixteenth Street, NW
Washington, D.C. 20005
Telephone: (202) 626-5800
Facsimile: (202) 626-5801
Email: kbehre@milchev.com
totoole@milchev.com
lbriggerman@milchev.com
iherbert@milchev.com
clee@milchev.com
cmarden@milchev.com

Attorneys for Plaintiff Farhad Azima

CERTIFICATE OF WORD COUNT

The undersigned certifies compliance with Local Rule 7.3(d) regarding length limitations. This memorandum contains fewer than 6,250 words. The undersigned has relied on the word count feature of Microsoft Word 365 in making this certification.

This, the 14th day of August, 2024.

/s/ Ripley Rand
Ripley Rand
Counsel for Plaintiff

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-cv-954-WO-JLW

FARHAD AZIMA, Plaintiff, v. NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC., Defendants.	**CERTIFICATE OF SERVICE**

I hereby certify that I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send electronic notification of this Notice to the following attorneys:

Brandon S. Neuman, Esq.
Jeffrey M. Kelly, Esq.
NELSON MULLINS RILEY & SCARBOROUGH, LLP
301 Hillsborough Street, Suite 1400
Raleigh, NC 27603
brandon.neuman@nelsonmullins.com
jeff.kelly@nelsonmullins.com
Tel.: (919) 329-3800
Fax.: (919) 329-3799

Samuel Rosenthal
NELSON MULLINS RILEY & SCARBOROUGH LLP
101 Constitution Ave. NW, Suite 900
Washington, DC 20001
sam.rosenthal@nelsonmullins.com
Tel.: (202) 689-2951
Fax: (202) 689-2860

Justin B. Kaplan
George C. Mahfood
NELSON MULLINS RILEY & SCARBOROUGH LLP
2 South Biscayne Blvd., 21st Floor
Miami, FL 33131
justin.kaplan@nelsonmullins.com
george.mahfood@nelsonullins.com
Tel: (305) 373-9400

Counsel for Defendants

This, the 14th day of August, 2024.

WOMBLE BOND DICKINSON (US) LLP

/s/ Ripley Rand
Ripley Rand
North Carolina State Bar No. 22275
555 Fayetteville Street, Suite 1100
Raleigh, NC 27601
Telephone: (919) 755-8125
Facsimile: (919) 755-6752
Email: ripley.rand@wbd-us.com

Counsel for Plaintiff